Managed Mobile Device Email Security Configuration

The purpose of this document is to list and explain the settings of the Exchange Security Configuration (ESC) for your managed mobile device when it connects to the State of Montana's Microsoft Exchange mobile device connection interface.

For a definition of a managed mobile device or to find out more information about the E-MAIL MOBILE service, go to the Service Catalog located on the MINE Portal.

I. General Information

An ESC policy has been implemented for all managed mobile devices that connect to the State's Exchange email system. The ESC only affects managed mobile devices that are running compatible software and connecting to the Exchange mobile device connection interface.

The DOA ITSD responsibility is limited to verification that the mobile device connection interface is up and available and that a DOA ITSD test mobile device can use the mobile device connection interface. DOA ITSD WILL NOT provide troubleshooting or support for my unmanaged mobile devices.

Support of the managed mobile device is provided by the mobile device provider or other agency designated staff.

Not all mobile devices can fully implement the security and configuration changes outlined in this document concerning the ESC. When a mobile device cannot fully implement the ESC some features may not work correctly or the mobile device may have reduced security. It is the customer's responsibility to test their mobile device when using the E-MAIL MOBILE service to ensure it meets their security and feature requirements.

II. ESC Password Settings

A. **Password:** To comply with Enterprise Security Policy -063 (ENT-SEC-063), users shall select passwords of at least 6 characters, containing at least one alphabetic and one numeric character. Passwords will expire after 60 days. A password may not be reused until six password changes have been made.

B. **Password Attempts:** The number of failed password attempts allowed will be 8. **After the 8th attempt, the mobile device will hard wipe, erasing all data on the device, including storage devices.** Your managed mobile device will then be set back to factory defaults. There is no password attempt reset interval; so, if you enter the password incorrectly 3 times and wait one hour, you will still have 3 failed attempts. On the 5th incorrect password attempt, you will be asked to type in an alpha-numeric phrase displayed on the screen in order to continue. This precaution is to ensure your password is actually being entered by a user and not by random button presses**.**

C. **Managed Mobile Device Idle Time Out:** Users will be required to re-enter their password if more than 15-minutes of idleness have elapsed.

III. ESC Removable Storage Media Encryption

A. The ESC will require that all removable storage media attached to your device be encrypted. Common examples of removable storage media are Compact Flash cards, Secure Digital (SD) cards, and micro USB flash drives. If your managed mobile device is wiped, then the removable storage device will become inoperable until you format the media again. After the storage device is reformatted, it will be usable again.

B. The encryption of the removable storage device applies to all data saved to the removable storage device via the managed mobile device. You will not be able to insert the removable storage device into another mobile device or computer and retrieve the encrypted data. If you put data on the removable storage device from a computer, these files will not be encrypted until they are opened and saved on the removable storage device using the managed mobile device.

C. The user is responsible for backup of all data on the managed mobile device and on the removable storage media. If the managed mobile device is wiped or reset, the ability to decrypt the data is lost, and all of the data stored on the removable storage device is no longer accessible.